



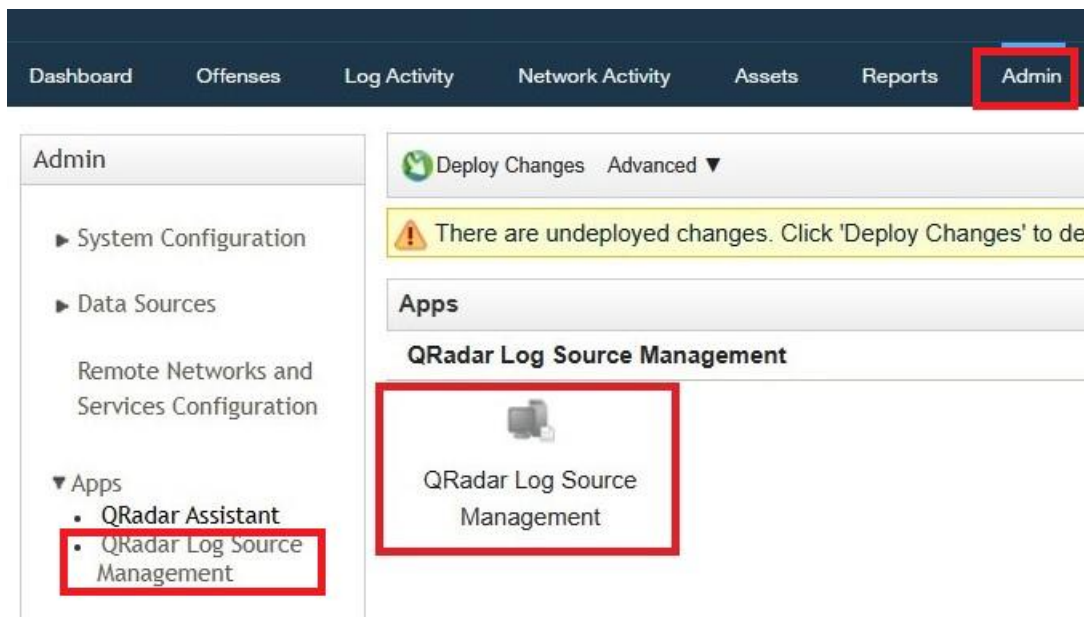
QRADAR INTEGRATION

AppSentinels API Security Platform supports QRadar integration for the Security Events/Vulnerability Events using public APIs and using QRadar Universal CloudRest API.

The following steps has to be followed to configure the QRadar to fetch the events in regular interval.

1 Select Log Source Management

- Go to Admin -> QRadar Log Source Management
- Open the QRadar Log Source Management



2 Configuration New Log Source

Configure “New Log Source” to add AppSentinels events source.



Choose Single Log Source



3 Select Log Source TYPE

Select “Universal DSM” as the Log Source Type

IBM QRadar Log Source Management - Add a Single Log Source

- Select Log Source Type
- Select Protocol Type
- Configure Log Source Parameters
- Configure Protocol Parameters

Select a Log Source type

Univ

- Universal CEF
- Universal DSM**
- Universal LEEF

Step 2: Select Protocol Type

4 Select Protocol Type

Select “Universal Cloud REST API” as protocol type

IBM QRadar Log Source Management - Add a Single Log Source

- Select Log Source Type
- Select Protocol Type
- Configure Log Source Parameters
- Configure Protocol Parameters
- Test Protocol Parameters

Select a protocol type

Look up Protocol Type

- OPSEC/LEA
- Oracle Database Listener
- SDEE
- SMB Tail
- SNMPv1
- SNMPv2
- SNMPv3
- Sophos Enterprise Console JDBC
- Sourcefire Defense Center Estreamer
- Syslog
- Syslog Redirect
- Universal Cloud REST API**

Step 1: Select Log Source Type

Step 3: Configure Log Source Parameters

5 Configure Log Source Parameter

5.1 Configure the Log Source Parameters

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Configure the Log Source parameters

Name *
The name of the log source.

AppSentinels

Description
An optional description of the log source.

AppSentinels API Security Platform

Enabled
Indicates whether the log source should be enabled.

☒ On

Groups *
The groups that this log source will belong to.

Other X

Q + Add Group

Extension
Log Source Extensions perform post-processing of events after default parsing has

Select...

Step 2: Select Protocol Type

Step 4: Configure Protocol Parameters

5.2 Update the workflow and workflow parameters. Refer the section Workflow Details section for details.

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Configure the protocol parameters

Log Source Identifier *

AppSentinels

Workflow *
The XML document that defines how the protocol instance collects events from the target API.

```
<?xml version='1.0' encoding='UTF-8'>
<Test>
  <HTTPConnectionThroughProxyTest url="https://{/host}" />
</Test>
</Workflow>
```

Workflow Parameter Values
The XML document that contains the parameter values used directly by the workflow.

.....

Allow Untrusted Certificates
Enable this option to allow self-signed or otherwise untrusted certificates.
[+ Show More](#)

☐ Off

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

5.3 Configure the Protocol Parameters “Collect Events Count” as 100 (AppSentinels Platform provides maximum 100 events in response) and “Collect Events Duration” with the interval in secs to fetch the Security Events

IBM QRadar Log Source Management - Add a Single Log Source

- Select Log Source Type
- Select Protocol Type
- Configure Log Source Parameters
- Configure Protocol Parameters
- Test Protocol Parameters**

Test Protocol Parameters

Test this log source configuration to ensure that the parameters are correct.

The test runs from the host specified by the Target Event Collector parameter. If there is high network latency, it may take a moment for the results to appear.

The test collects sample event data from the target system. This feature can be disabled in the settings.



Start Test

Settings

Collect Events ☒ On

Collect Events Count

Collect Events Duration

Show Debug Messages ☐ Off

Step 4: Configure Protocol Parameters

Skip Test and Finish

5.4 Test the configuration to confirm the events are retrieved by QRadar

IBM QRadar Log Source Management - Add a Single Log Source

- Select Log Source Type
- Select Protocol Type
- Configure Log Source Parameters
- Configure Protocol Parameters
- Test Protocol Parameters**

Test Protocol Parameters

Restart

Results (3):

- Testing DNS resolution of [in-cloud.appsentinels.ai]
- Testing TCP connection to [in-cloud.appsentinels.ai:443]
- Testing SSL connection to [in-cloud.appsentinels.ai:443]

Events (100):

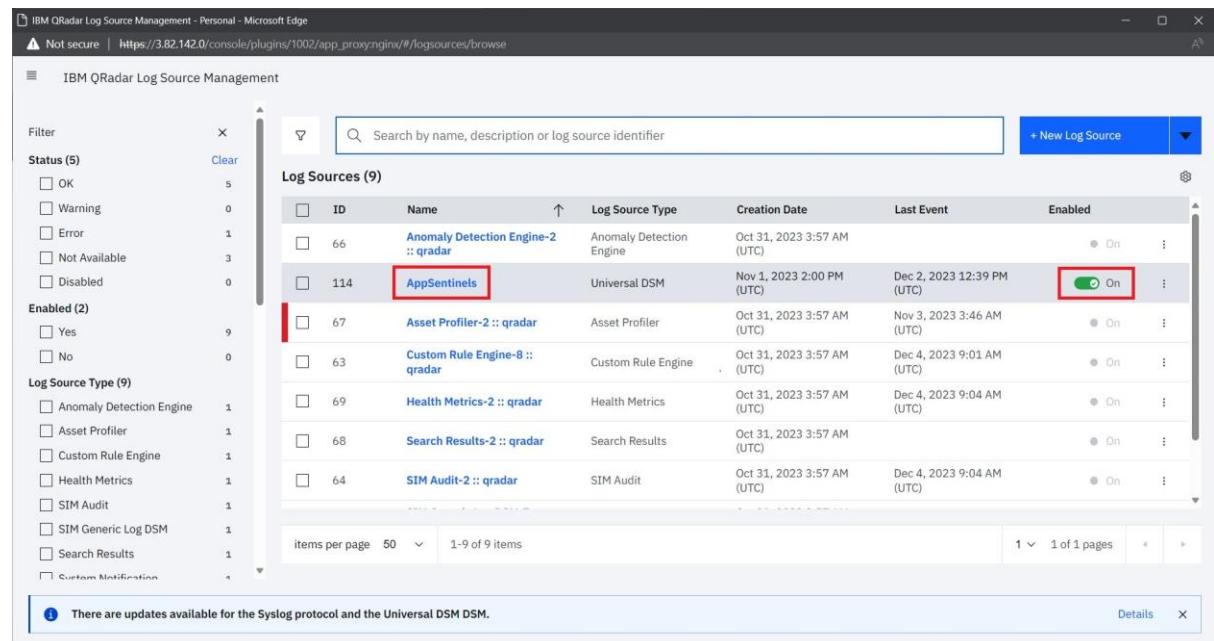
Log Source Identifier	Payload
AppSentinels	{"action": "log", "api_info": {"Request Body": {}, "Request Header": [{"user-agent": "Mozilla/5.0 (Macintosh; Intel Mac OS version 10_0_0; rv:42.0) Gecko/20100101 Firefox/42.0"}]}}
AppSentinels	{"action": "log", "api_info": {"Request Body": {}, "Request Header": [{"user-agent": "Mozilla/5.0 (compatible; Nmap Script Engine/0.92)"}]}}
AppSentinels	{"action": "log", "api_info": {"Request Body": {}, "Request Header": [{"user-agent": "Mozilla/5.0 (compatible; Nmap Script Engine/0.92)"}]}}

Step 4: Configure Protocol Parameters

Finish

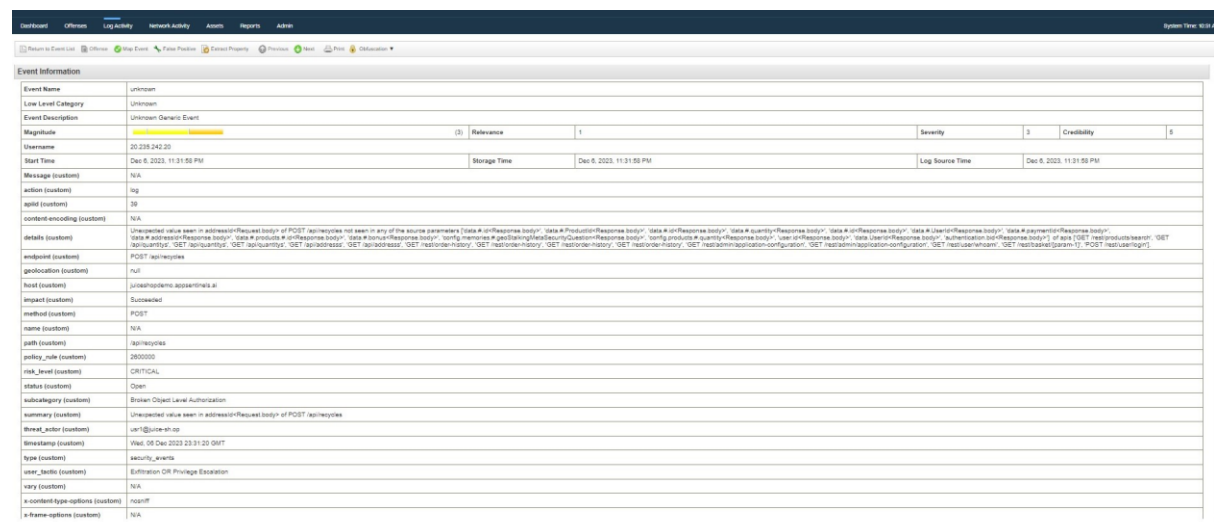
6 Confirm Log Source is added

AppSentinels should be listed in the Log Sources list and should be enabled.



7 Verify Events in JIRA

Generate Security events and verify the Security Events are retrieved by QRadar.



8 Mapping of Events field

AppSentinels Security Events fields uses API Security related parameters in the event details. Use the DSM Editor to map the AppSentinels Event parameters with standard fields of QRadar.

9 Workflow Parameters Details

AppSentinels has defined the workflow.xml and workflow.parameters.values.xml required for integrating AppSentinels API Security Platform events to QRadar.

The files can be downloaded from <https://storage.googleapis.com/appsentinels-deployment/index.html>

9.1 AppSentinels_workflow.xml

The severity of the events to be fetched should be updated in the appsentinels_workflow.xml file. The supported severity values are critical, major, minor and info.

```
<RequestHeader name="Accept" value="application/json" />
<RequestBody type="application/json" encoding="UTF-8">{"include_runtime_scan": ${/include_runtime_scan}, "last_event_id": ${/last_event_id}, "severity": ["critical", "major"], "type":
"${/type}", "aggregation": ${/aggregation}}</RequestBody>
```

9.2 AppSentinels_workflow.parameter.values.xml

```
<?xml version="1.0" ?>
```

```
<WorkflowParameterValues
```

```
xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/WorkflowParameterValues/V2">
```

```
  <Value name="host" value="in-cloud.appsentinels.ai"/>
```

```
  <Value name="apiKey" value="APIKEY"/>
```

```
  <Value name="orgName" value="ORGNAME"/>
```

```
  <Value name="appName" value="ORGNAME_APPNAME"/>
```

```
  <Value name="include_runtime_scan" value="false"/>
```

```
  <Value name="aggregation" value="true"/>
```

```
  <Value name="type" value="security_events"/>
```

```
</WorkflowParameterValues>
```

apiKey: API KEY generated in the AppSentinels Platform for accessing the public APIs

orgName: Organization Name as defined in the AppSentinels Platform

appName: Application Name as defined in the AppSentinels Platform

include_runtime_scan: To include the vulnerability events from the run time scan category. This configuration is applicable to vulnerability events.

aggregation: To fetch only the parent attack or fetch all the attacks when the similar events are aggregated.

type: Type of the event, could be security_events or vulnerabilities